An introduction to **CBEST**

Background

Existing penetration testing services conducted within the financial services sector are well understood and utilised. While these services have provided a good level of assurance against traditional capability attacks, it is becoming increasingly clear that they do not provide assurance against more sophisticated attacks on critical assets. There are two main reasons for this. The first is that the financial services sector has resisted testing critical assets against simulated attacks because of the perceived associated risk. The second is that the penetration testing industry did not have sufficient access to current and specific threat information.

In 2013, the Financial Policy Committee issued a recommendation to HM Treasury requesting that they and regulators work with the core UK financial systems and the infrastructure providers that support them, to put in place a programme of work to improve and test resilience to sophisticated cyber attacks. The Committee also noted it was important that boards of financial firms and infrastructure providers recognised their responsibility for responding to attacks, which requires a combination of continuous vigilance and investment to strengthen operational resilience.

As a result, the UK Financial Authorities - Bank of England (BoE), Her Majesty's Treasury, and the Financial Conduct Authority - have taken steps to address these issues. They have consulted with financial services organisations, while also working with the penetration testing and cyber threat intelligence services industry to develop a scheme that is sympathetic to the concerns raised by the financial services industry and the risks associated with testing critical assets.

It is through these consultations that the Financial Authorities have defined the CBEST testing framework. The implementation of CBEST will help the boards of financial firms, infrastructure providers and regulators to improve their understanding of the types of cyber attack that could undermine financial stability in the UK, the extent to which the UK financial sector is vulnerable to those attacks and how effective the detection and recovery processes are. CBEST, with the support of industry, puts in place measures to ensure that targeted tests can be conducted on critical assets without harm.

What Is CBEST?

CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

CBEST differs from other security testing currently undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks on critical systems and essential services. CBEST provides an holistic assessment of a financial services or infrastructure provider's cyber capabilities by testing people, processes and technology in a single test which will be less time constrained than traditional penetration testing.

The inclusion of specific cyber threat intelligence will ensure that the tests replicate, as closely as possible, the evolving threat landscape and therefore will remain relevant. CBEST will utilise key performance indicators to measure capability and maturity in this important area and provide benchmark information to the industry and regulators. This benchmark information will not only improve the position of those that have been subject to CBEST but will also help to inform where effort needs to be focussed to improve all aspects of the financial services industry's ability to protect itself from cyber attacks and to be able to detect and respond appropriately.

To ensure the test is safe but also realistic, new accreditation standards have been developed with CREST, the not-for-profit organisation that represents the technical information security

CBEST

CREST STAR

industry. These standards augment the already stringent standards that CREST demands and require security testing companies to demonstrate that they have policies and processes in place to manage and conduct CBEST activities. They also assess the extremely high levels of technical knowledge, skill and competency required by the individuals directly involved in CBEST activities.

For the first time CREST requires commercial intelligence providers to be accredited, ensuring financial services and infrastructures providers have access to detailed, considered and consistent cyber threat intelligence that has been ethically and legally sourced. The CBEST framework ensures that security testers and threat intelligence providers work together, replicating very real attacks from sophisticated adversaries. Both the companies providing CBEST services and those qualified to conduct the work are bound by detailed, relevant and enforceable codes of conduct administered by CREST.

Benefits to the financial sector

CBEST has the full support of the UK Financial Authorities and will provide significant benefits to the UK's financial sector. These include:

- access to considered and consistent cyber threat intelligence, ethically and legally sourced from organisations that have been assessed against rigorous standards;
- access to knowledgeable, skilled and competent cyber threat intelligence analysts who have a detailed understanding of the financial services sector;
- realistic penetration tests that replicate sophisticated, current attacks based on current and targeted cyber threat intelligence;
- access to highly qualified penetration testers that understand how to conduct these technically difficult testing activities while ensuring that no damage is caused;
- confidence in the methodologies utilised by the companies within CBEST for conducting these sophisticated and sensitive tests;
- confidence that the results and the information accessed by the testers will be protected;
- standard key performance indicators that can be used to assess the maturity of the organisation's ability to detect and respond to cyber attacks;
- access to benchmark information, through the key performance indicators, that can be utilised to assess other parts of the financial services industry;
- a framework that is underpinned by comprehensive, enforceable and meaningful codes of conduct administered by a specialist professional body.

The validation of the threat intelligence and penetration testing services companies' policies, processes and procedures and the requirement to validate the skill, knowledge and competence of the individuals bound under enforceable codes of conduct, provide financial services companies with a very high level of assurance in the services provided under CBEST. These services can also be utilised by the financial services companies for self-initiated tests of their critical systems and services and are applicable to other key sectors.

Choosing a suitable supplier

Details of CBEST approved cyber threat intelligence service suppliers and penetration testing companies can be found on the CREST website, **www.crest-approved.org**. These organisations will be described as being CREST STAR members. Additional information on all aspects of CBEST and STAR is also available on the website.

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: crest-approved.org